REMARKS

This amendment is being filed as a response to the Office Action of August 21, 2008. Reconsideration is respectfully requested in view of these clarifying amendments and remarks.

Rejections under 35 USC § 103(a)

Claims 1-7, 9-12 and 15-19 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Falkenhaimer et al. (US Patent No. 5,930,801), in view of Chang et al. (U.S. Patent No. 6,157,953), in view of Levergood et al. (US Patent No. 5,708,780), and further in view of Gold et al. (US Patent Application 2002/0194326). This rejection is respectfully traversed. Applicants respectfully request reconsideration of these rejections in light of the amendments and arguments contained herein.

Independent claims 1, 9, 10 and 15 define checking for an account limitation to determine if a maximum number of accounts created has been reached (emphasis added). The Office has asserted that this feature is taught by Gold in the following paragraph:

> "[0050] Referring to FIG. 3 herein, there is illustrated schematically overall process steps carried out by capacity management application 208 for enforcement of user admission to the computer entity. Every time a new user account is added to the computer entity in process 300, and even where no new user accounts are added, every time a pre-determined maintenance period occurs in process 301, a user capacity limiting algorithm 302 is run. The capacity limit algorithm operates on the basis of a number of "user accounts", which in the case of a network attached storage device are client backup accounts. The capacity limit algorithm prevents too many users being installed on the computer entity which would result in using up all the available licensed data storage capacity. The capacity limit algorithm is run by the computer entity on a regular basis, for example whenever a new user account is stored plus once per day, at the end of a nightly data maintenance job. The capacity limit algorithm determines a predicted capacity growth trend for user accounts currently installed on the computer entity and then calculates how much currently available licensed data storage capacity is used by each currently installed user account, assuming a look ahead growth period from the installation date of each user account. Typically the look ahead period will be set to predict in advance for a pre-determined period, for example two years growth from the installation date of each user account. Where a user account

> has not been installed long enough to predict a capacity usage trend data, then default values, generated from a sample of typical user accounts, may be used to assign a predicted capacity growth trend to that user account. Each time the capacity limit algorithm is run, it produces as an output a value of predicted growth requirement, in units of megabytes. Depending upon the current number of user accounts assigned to the computer entity, and their predicted capacity growth requirement in megabytes, the capacity limit algorithm either prohibits entry of new user accounts, or allows entry of new user accounts" (parg. [0050] - emphasis added).

Applicant respectfully disagrees. Gold teaches allowing new user accounts based on the predicted capacity [storage] growth requirements and not based on a maximum number of accounts, as claimed by Applicant. See also step 504 in Fig. 5 of Gold. Predicted storage growth depends on how the different accounts are predicted to use storage. A given system may predict a large use of storage data per user, resulting in less users, while other system may predict a small amount of storage data per user, resulting in more user accounts permitted for a same level of storage. That is, predicted storage use is not the same as a maximum number of users, as different systems will predict different levels of storage use for the same amount of user accounts. Thus, allowing new user accounts based on predicted capacity, as in Gold, does not teach checking for an account limitation to determine if a maximum number of accounts created has been reached, as claimed by Applicant.

Additionally, claim 1 has been amended to define requesting the account from a requestor on a client, the requestor being activated through administrator action (emphasis added). There is no teaching in Falkenhaimer of a requestor in the client, as asserted by the Examiner "user can create to request an account" (page 3, second to last paragraph). The user requests the account directly from [remote] command utility 18, as seen in Fig. 1, but the user does not request the account from the requestor on a client, as claimed by Applicant. Consequently, Falkenhaimer does not teach that the requestor is activated through administrator action either, thus present claim 1 is believed to be patentable.

Further, claim 9 has been amended to define receiving the account request from a software agent (emphasis added). Falkenhaimer teaches a user requesting an account, as described previously, but there is not teaching in the prior art of a software agent originating the account request. Thus, present claim 9 is believed to be patentable.

Still yet, claims 10 and 15 have been amended to incorporate subject matter from former claim 16 and define a network attached storage (NAS) device coupled to the connector, the NAS device being capable of storing the account (see this or similar, but not necessarily identical language in Claims 14 and 26 - emphasis added). In the rejection of former claim 16, the Office has asserted that Falkenhaimer teaches this feature in Fig. 1 and the following excerpt:

> "When a user account is created, a utility within command utility 18 called a "community registry" creates a new object which includes data describing the user. The registration process includes the user filling out an electronic form, data from which is used in the user object. Such user information can include, for example, the user's legal name, hard-copy and e-mail addresses, website URL, and the names of user groups he wishes to be associated with (this is equivalent of naming "parent" collections for the user, assuming the user groups have handles and objects associated therewith, and may be subject to security considerations). Also, preferably, at this point the new user will be asked to type in a password he will use for future logins to the system. The password will be checked by the command utility 18 at all future times the user logs into the system" (col. 8, line 66 - col. 9, line 13, emphasis added).

There is no mention in the excerpt reference by the Office that teaches a network attached storage (NAS), much less a NAS device coupled to the connector, the NAS device being capable of storing the account. Further, Figure 1 includes "a file system 12, which may be in the form of, for example, a hard-drive or network server" (col. 2, lines 57-59, emphasis added). A hard drive or network server do not teach a NAS device couple to the connector

and being able of storing the user account. Thus, claims 10 and 15 are believed to be patentable for at least these reasons.

In view of the foregoing, the Office is requested to withdraw the rejection of claims 1, 9, 10, and 15 under §103. The dependent claims are submitted to be patentable for at least the same reasons the independent claims are believed to be patentable. The Applicants therefore respectfully request reconsideration and allowance of the pending claims. A Notice of Allowance is respectfully requested.

If the Examiner has any questions concerning the present amendment, the Examiner is kindly requested to contact the undersigned at (408) 774-6920. If any other fees are due in connection with filing this amendment, the Commissioner is also authorized to charge Deposit Account No. 50-0805 (Order No. ADAPP256).

Respectfully submitted,
MARTINE PENILLA & GENCARELLA, LLP

/Jose M. Nunez/

Jose M. Nunez
Reg. No. 59,979

710 Lakeway Drive, Suite 200
Sunnyvale, CA 94085
Telephone: (408) 749-6900
Facsimile: (408) 749-6901
Customer Number 25920